

# Copyright Violations

---

## Table of Contents

1. Introduction.....	1
2. Bandwidth .....	1
3. Copyright complaints and legal content alternatives.....	1
4. Training Resources .....	2
5. Peer-to-peer software .....	2
6. Revision History .....	3
7. Approvals.....	3

## 1. Introduction

**Using peer-to-peer (P2P) file-sharing applications to illegally share copyrighted music and movies is the #1 way students violate federal copyright law.** Students, faculty and staff are all obligated to comply with federal law and university policy regarding appropriate use of information technology and avoiding copyright infringement.

## 2. Bandwidth

The university enforces network policies regarding [bandwidth usage and limits](#). Under some circumstances, the university may activate monitoring tools designed to detect abnormal or potentially infringing traffic in order to determine its appropriateness and, if necessary, initiate disciplinary procedures.

## 3. Copyright complaints and legal content alternatives

If you copy and distribute copyrighted material without legal permission, you may be found liable for civil or criminal copyright infringement. Civil penalties for Federal Copyright infringement range from \$750 per song to \$150,000 in damages for each willful act. Criminal penalties can run up to five years in prison and \$250,000 in fines. Student Judicial Services administers penalties and sanctions in accordance with Chapter 11 of the Institutional Rules on Student Services and Activities and Rule 50101 of the Board of Regents Rules and Regulations.

The university cannot protect you from a copyright complaint. The university may also be required by law to disclose information about you to a complainant for use in pursuing legal action against you. The

## **Copyright Violations**

**Document Version:** Approved

process for handling DMCA notices received by the university is outlined in the [Digital Millennium Copyright Act](#) (DMCA) policy. The penalties for violation of copyright law can range from university sanctions to civil and criminal prosecution. Refer to Student Legal Services' article on [Notice of Illegal Music Downloading and File Sharing from the RIAA or MPAA](#), and read more about [Enforcement Activities by Copyright Holders](#).

You are not protected from financial penalty just because you received material at no cost or are distributing material with no charge. Your only protection is to not possess or distribute any unlicensed copyrighted material. There are many Web sites that provide legal online music, movies, and other content. Refer to the [Keep It Legal](#) page for a list of services that comply with the DMCA.

## **4. Training Resources**

- Faculty and staff are required to take [IT Security Awareness training](#) every two years.
- Students are required to take [IT Security Awareness training](#) when they first start at UT Austin.
- Students who exceed their bandwidth allowance can take an additional [Bandwidth Awareness for Students](#) course.
- UT System [Copyright Crash Course](#)
- [2009 Cybersecurity Awareness Campaign](#)
- [2008 Cybersecurity Awareness Month \(CSAM\) Campaign](#)
- [2007 CSAM Campaign](#)
- [2006 File Sharing Poster](#)
- [The Perils of Peer-to-Peer File Sharing](#)

## **5. Peer-to-peer software**

Peer-to-peer (P2P) applications such as BitTorrent, BearShare, Limewire, Morpheus, iMesh and KaZaA make it easy for you to share files, and there are legitimate uses for this class of software. However, please keep the following guidelines in mind.

### **5.1. Network bandwidth**

Most P2P applications are configured so other users can access your hard drive and share your files all the time. This constant file transfer can degrade your computer's performance and generate heavy traffic loads on the university network. P2P applications can consume your weekly allocation very quickly.

The university's network bandwidth consumption is monitored. If your usage impacts the overall performance of the network, your computer may be blocked.

If you use a P2P application to share content legally, you should know how to [control or disable the application](#).

### **5.2. Privacy**

If you are running a P2P application, you may be inadvertently sharing personal information, such as e-mail messages or credit card information. You need to make sure you know which files and data the application is sharing. You should know how to [control or disable your P2P application](#) to ensure that you are not inadvertently sharing personal information.

### 5.3. Security

Viruses are easily spread using P2P applications. Many P2P applications include “malware” in the download, so you may be unintentionally infecting your computer. To protect your computer, keep your anti-virus program up-to-date and only install programs acquired from reputable sources. You can download anti-virus software on the [BevoWare site](#).

### 5.4. Resource Use

Some P2P applications use your computer as a computational or storage resource for another organization’s use. This may not be an acceptable use of state-owned resources such as the university network or university-owned computers. Do not permit any such use of your system without the consent of the university. For assistance, please contact the Information Security Office, [abuse@utexas.edu](mailto:abuse@utexas.edu).

### 5.5. University Policy and Assistance

By running a P2P application, you may be consuming excessive network bandwidth and/or violating copyright law, both of which are violations of the university’s [rules for acceptable use of information technology](#). You may also be sharing confidential information and/or making your computer insecure.

If you have questions about P2P applications, please call the [ITS Help Desk](#) at 512-475-9400 or send e-mail to [the ITS Help Desk](#).

## 6. Revision History

Version	Date	New	Original
<b>Copyright Violations.pdf</b>	08/02/2011	Created pdf from web page	

## 7. Approvals

Name	Role	Members	Date
<b>Cam Beasley</b>	Information Security Officer		09/15/2007